**Cybersecurity Identification Policy**

Revision: 1.0

Approved:

Date: 05/06/2024

**1. Introduction**

1.1. Purpose: The purpose of this cybersecurity identification policy is to establish procedures for identifying, categorizing, and managing information assets, business processes, and cybersecurity risks within the organization in alignment with the NIST Cybersecurity Framework (CSF) Version 2.0.

1.2. Scope: This policy applies to all employees, contractors, and third-party vendors who have access to the organization's information systems and data assets.

1.3. CISO – the person performing this role

**2. Asset Identification**

2.1. Information Assets:

* All information assets, including but not limited to data, systems, applications, networks, and devices, shall be identified and documented.
* Information assets shall be categorized based on their criticality, sensitivity, and importance to the organization's operations.

2.2. Business Processes:

* Critical business processes and functions shall be identified and documented, including their dependencies on information assets and technology systems.

**3. Risk Identification**

3.1. Cybersecurity Risks:

* Potential cybersecurity risks shall be identified through regular risk assessments conducted using the methodology outlined in the NIST CSF 2.0.
* Risks shall be categorized based on their likelihood, potential impact, and severity.
* Any changes to infrastructure or network flows will go through a change request workflow to access potential impact and ensure documents are kept up to date

3.2. Threat Intelligence:

* Threat intelligence sources shall be monitored to identify emerging cybersecurity threats and vulnerabilities relevant to the organization's industry and operations.

**4. Data Classification**

4.1. Data Classification Scheme:

* A data classification scheme shall be established to categorize data based on its sensitivity, confidentiality, integrity, and availability requirements.
* Data classification labels shall be applied consistently across all information assets and systems.

4.2. Handling Procedures:

* Procedures for handling and protecting data according to its classification level shall be defined and communicated to relevant personnel.
* Access controls and encryption mechanisms shall be implemented based on data classification requirements.

**5. Incident Identification**

5.1. Incident Detection:

* Mechanisms for detecting cybersecurity incidents, such as intrusion detection systems, security information and event management (SIEM) systems, and user activity monitoring, shall be implemented.
* An incident response team shall be designated and trained to respond to cybersecurity incidents promptly.

**6. Governance and Compliance**

6.1. Compliance Requirements:

* This policy shall comply with relevant cybersecurity laws, regulations, and industry standards applicable to the organization's operations.
* Compliance with this policy shall be regularly assessed through audits and reviews.

**7. Roles and Responsibilities**

7.1. Chief Information Security Officer (CISO):

* The CISO shall be responsible for overseeing the implementation of this identification policy and ensuring compliance with the NIST CSF 2.0.
* The CISO shall designate personnel responsible for asset identification, risk assessment, data classification, and incident identification.

7.2. IT Department:

* The IT department shall implement technical controls and tools for asset and incident identification, including asset management systems, network monitoring solutions, and security information and event management (SIEM) platforms.

**8. Training and Awareness**

8.1. Employee Training:

* All employees shall receive training on the identification and classification of information assets, cybersecurity risks, and incident detection procedures.
* Awareness programs shall be conducted regularly to keep employees informed about the importance of cybersecurity identification practices.

**9. Review and Revision**

9.1. Policy Review:

* This cybersecurity identification policy shall be reviewed and updated periodically to reflect changes in the organization's technology environment, business operations, and regulatory requirements.
* Reviews shall be conducted at least annually or more frequently as needed.

**Reference Documents**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |